平成23年度 卒業論文

論文題目

インターネット上における文字認証システムの問題点と具体的な解決方法の提案

神奈川大学 工学部 電子情報フロンティア学科

学籍番号　200803026

蓑和　玲

指導担当者　木下宏揚　教授

目 次

図 目 次

表 目 次

第1章

序論

近年、インターネットの普及により、インターネット上でのサービスが多くみられる。その中でも、ユーザーの登録を行い、ユーザーごとに情報を管理し、サービスの質の向上をしているものについては、使用者がその本人であるという証明のために認証が必要であり、その認証に、最も多く使われているのが、パスワードを用いた文字認証である。

しかし、その反面、アカウントハック（パスワードを何らかの方法で盗む、あるいは解析などをして損害を与える、もしくは利益を得る行為）などが大きな問題となっており、これについては、ユーザーのセキュリティに対しての関心、危機感が不十分であることが原因となっていると考えられる。

今回の研究では、ユーザーのセキュリティに対する考え方がどのようなものかを確認したうえで、それに対する具体的な対策方法を提案することを目的とする。

第2章

パスワードに関しての調査

2.1　良いパスワードとは

パスワードの良し悪しの基準として、以下のものが挙げられる

セキュリティ面から見た要素

・パスワードの長さ

・非連想、無機的

・文字種類の多様性

・他のアカウントとの非重複

ユーザーから見た要素

・覚えやすさ

・入力のしやすさ

この他に、状況によって、パスワードを変更することが求められる。

これらの要素についての調査結果は以下のとおりである。

・パスワードの長さ

当然ではあるが、長ければ長いほどセキュリティには有効である。ただし、長い場合、覚える手間や、入力の手間が増えることになる。大文字小文字、数字と記号を用いた場合、8 文字のパスワードであれば、通常のパソコンの処理能力ではブルートフォースアタック（総当たり攻撃）による解析時間は 23 年を超えるというデータがある。しかしこの数字は安心できるものではなく、処理能力の高いコンピュータや、並列処理が可能なコンピュータの数によっては短時間での解析が可能である。大文字 26 種、小文字 26 種、数字 10 種、記号 5 種程度であったとしても、パスワードが 1 文字増えることで考えられる組み合わせが 67 倍にもなるので、少しでも長いパスワードを設定すると良く、あくまで 8 文字は最低限、14 文字以上が理想であるという説もある。また、長いパスワードを設定することができない制限を設けているサイトが多いのも問題点の一つである。

・非連想、無機的

自分、あるいはその周囲の情報から推測されないこと。名前や誕生日をそのままパスワードとして設定するなどはもってのほかである。また、パスワード攻撃には、辞書攻撃というものがあり、辞書に存在する文字列を優先的に試す方法であり、何かの単語を組み合わせたパスワードでは、パスワードが長くても短期間で解析される恐れがある。可能な限り、意味を持たないパスワードを考案することが重要である。

・文字種類の多様性

パスワードには文字の種類（大文字、小文字、数字、記号）をまんべんなく使用することが望ましい。小文字のみを使用したパスワードとすべてを使用したパスワードでは 8 文字パスワードでも、可能な組み合わせが 680 億倍もの違いがある。それだけでなく、弱いパスワードでは攻撃の対象になりやすいことも問題である。

・他アカウントとの非重複

アカウントを複数持っている場合、そのすべてのパスワードが同一であると、1 つのパスワードが解析されたときに、ほかのアカウントも解析されてしまう。このような事態を避けるために、アカウントごとにパスワードは変えておくのが無難であると考えられる。

・覚えやすさ.

良いパスワードを作成したとしても、それを暗記できず、メモなどに書いたのでは良いパスワードを作成した意味がない。無機的で長いパスワードは覚えることが困難で、パスワードの変更が必要な場面でも覚えなおす手間がある。

・入力のしやすさ

長いパスワードの場合、入力の手間がかかるだけでなく、携帯端末などの入力方法に制限がかかる状況においても入力が容易なパスワードが望まれる。

・パスワードの変更

定期的にパスワードを変更することが望まれる、とされてきたのだが、近年では、難解なパスワードを使い続けるほうがよいという声が強い。新しくパスワードを作成した場合、新たなパスワードを考える手間があり、それを覚える時間も必要である。無機的なパスワードを作成した場合、そのパスワードを完全に覚えるまでに2/3程度の人が30日ほどかかり、この状態で新しいパスワードを定期的に考えようとすると、弱いパスワードを作ってしまう人が多くなると考えるのが妥当である。なので、パスワードを変更することを考えず、難しいパスワードを使用し、覚えて使うというのが必要である。ただし、攻撃を受けた形跡がある場合などはパスワードを変更するのが良いと思われる。

セキュリティ面から見た要素と、ユーザーから見た要素がトレードオフの関係になっていることは明白であり、この相違を埋めるシステムを考える必要があるといえる。

2.2 パスワードに関しての意識について

現状、パスワードに対しての危機意識は一般的に低いものと考えられる。米SplashDate社が発表した2011年の「最悪なパスワード」では、1位にPassword、2位に123456、などといった結果が示されていて、攻撃耐性の強いパスワードを作ろうという考え方そのものが無い人も居るということがこの結果から窺い知ることができる。また、日本の衆議院ではサイバー攻撃を受けたにもかかわらず、パスワードの変更を行った議員は半数に満たないなど、意識の低さが浮き彫りとなっている。これらの意識の低さを、前述の覚えやすさや入力のしやすさが由来しているものの一部だと考え、難しいパスワードの作成を補助し、覚えやすく、入力しやすく、また面倒のない方法を提案することが重要であると考えた。

第3章

具体的な提案方法

今回提案する方法は、パスワードの入力を変換して、出力させる方法である。変換を行うため、変換前の入力、すなわちユーザーが入力するワードにセキュリティを求める必要はなく、機械的に変換を行うため、実効パスワードは無機的な文字列であり、セキュリティを確保することが可能であるため、セキュリティとユーザーの需要を両立することが可能であると考えた。
変換に用いるアルゴリズムは、アスキーコードを用いるなどいくつか考えられるが、固有性、利便性を考慮し、図1に示すアルゴリズムを提案する。

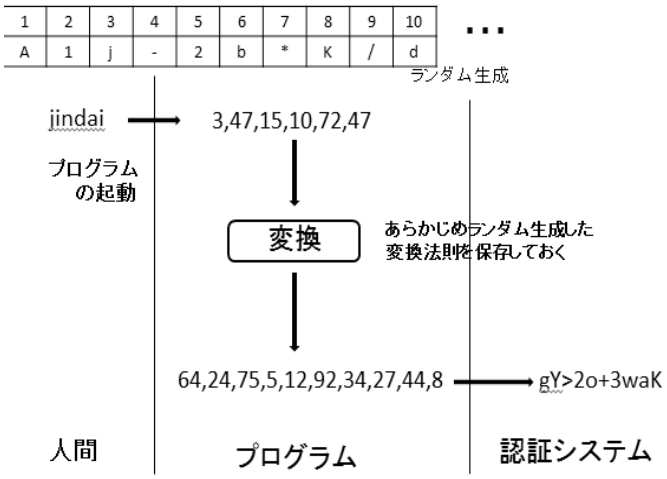

図 3.1　変換アルゴリズム

このアルゴリズムでは、文字列と数字を一意に対応させた表を用いて、入力した文字列を数字に変換して演算する。その結果を文字列に直すことで、無機的な長いパスワードに変換する。対応表は初回起動時に作成させるため、ユーザーごとに異なり、固有性が確保できる。また、演算の内容もそれぞれ別途に生成することで、異なるアカウントやパスワードの変更といったニーズにも対応することが可能である。さらに演算法則の指定に条件を付け加えれば、文字数の指定や、使用できない記号を指定することも可能になるといった利点がある。これらは前述したアスキーコードによる変換では実現できないため、このアルゴリズムに有効性があると考えられる。

また、今回の研究ではパスワードだけでなく、認証時に必要となるアカウント ID を取得し、組み合わせて変換する。このため、ユーザはアカウントごとに変換内容を作成する必要がなくなり、ユーザに負担をかけることなく、アカウントごとに別のパスワードを用意するというセキュリティ要件を満足しやすい構成を実装する。

第4章

基礎知識と今回使用する技術の解説

4.1　M系列

M系列とは、疑似ランダム系列の1つであり、疑似ランダム系列の中での有名なものの1つである。疑似ランダム系列とは、実際のランダム系列のような性質を持ちながら、同じ入力に対して同じ系列を生成する系列であり、簡単なシフトレジスタによって生成が可能であるため、幅広く使われているランダム系列である。
特にM系列には以下のような特徴がある。
・0と1の二進数で表される
・一定の長さの2値系列が連なった系列である
・周期の系列の長さはシフトレジスタのセル数の二乗に比例する。

4.2　線形帰還シフトレジスタ(Linear Feedback Shift Register,LFSR)

線形帰還シフトレジスタは、前述のM系列を生成するための手法の一つである。図2に示すようにシフトレジスタの初期値（入力データ）のうち、特定の一部を抽出し、排他的論理和を求める。求めた排他的論理和を左端のセルの入力とし、残りのデータを右にシフトさせる。この動作を繰り返すことによって、M系列を生成することができる。理論が単純であるため、ソフトウェア、ハードウェアとしても実装が簡単で、高速であることから幅広く使用されている。主に疑似乱数生成、疑似ノイ

ズ生成、高速デジタルカウンタ、白色化などの用途に用いられる。今回の研究では入力データを変換する目的で用いる。

4.3 メルセンヌ・ツイスタ法

メルセンヌ・ツイスタは帰還シフトレジスタを元にして作られた疑似乱数生成器であり、以下の特徴を持つ。

・2 の 19937 乗-1 という非常に長い周期をもつ。

2 の 19937 乗-1 という数字は名前の由来となっているメルセンヌ素数であり、このアルゴリズムの持つ特徴の一部は、内部的にメルセンヌ素数を用いていることに由来する。また、実際の運用上、これより長い周期をもつ疑似乱数を使用する理由はない。

・高次元（623 次元）に均等分布する

このことは連続して出力される値同士の相関性が無視できる程度であることを意味している。そのため、短い Bit 数の乱数を数回出力させ、長い Bit 数の乱数として使用しても統計的に安全である。

・長周期を生成する乱数生成器の中でも比較的高速である

・出力されるビット列は統計的に十分ランダムである。

・暗号論的な疑似乱数生成器ではない

メルセンヌツイスタは線形漸化式によって与えられるため、予測が可能である。暗号として用いるには暗号学的ハッシュ関数などの不可逆変換をすべきであるが、今回は単に乱数の生成として用いるため考慮する必要はない。

・内部ベクトルが大きいため、メモリの使用量が多い

・初期入力に 0 が多いとしばらくの間の出力が 0 に偏る

以上の特徴から乱数の生成に適していると考え、今回はプログラムの乱数生成として用いる。

第5章

結論

今回は利用者が所得しているオブジェクトとそれに関係しているなんらかのオブジェクトを所得して, 尚且つ利用者がそれを結び付けることが可能な推論規則を所得しているときに, 秘密情報が流出してしまうことを考慮した上でオブジェクト同士の関係を視覚化するシステムをオブジェクトを Node、オブジェクトに存在する関係を Edge を用いたグラフ構造で提案した.

あらかじめ推論規則など与えられていることを前提でシステム提案をしているがオブジェクトとそれを結ぶ関係の視覚化には成功した. 今後の課題としては推論規則自体も一つのオブジェクトとして見なすことも可能なので, もし推論規則をオブジェクトとしてみなした場合にどのように処理をすべきかの検討. そして外部ファイルとしてオブジェクト関係を入力できるかの検討などがある.

謝辞

本研究を行なうにあたり，終始熱心に御指導していただいた木下宏揚教授と鈴木一弘助手に心から感謝致します．また，公私にわたり良き研究生活を送らせていただいた木下研究室の方々に感謝致します．

2010年2月

鈴木　遼

参考文献

[1] ”情報漏洩について考えるサイト”
http://jouhourouei.j-nic.co.jp/index.html

[2] ”酒井剛典, 森住哲也, 畔上昭司, 小松充史, 稲積泰宏, 木下宏揚：“ Covert Channel 分析メカニズムと EJB による情報フィルタの構築 ”,2006 年暗号と情報セキュリティシンポジウム, (2006).”

[3] 森住哲也, 木下宏揚：“ 社会システムの中の Covert Channel について ”, 技術と社会・倫理研究会，(2005).

[4] ストレージネットワーク用語集 2008
http://www.snia-j.org/dictionary/

[5] 内野雄策:”SNS における情報漏洩を防止するための情報フィルタの適用 (2009)”

[6] ”ウィキペディア（Wikipedia)”
http://ja.wikipedia.org/wiki/

[7] ”株式会社ミクシィ”
http://mixi.jp/

[8] ”OR 事典” ”http://www.weblio.jp/cat/academic/orjtn”

[9] 高須忠和, 橋本健二, 石原靖哲, 藤原融: ”XML データベースへの型推論を用いた攻撃に対する安全性検証 (XML),(2006)”

質疑応答

Q1:発表に使われていた動画のノードが最初被っていたのは特に意味があるのか.また、動かせることのメリットは何か.(松澤教授)

A1:ノードが被っていたのはノードの配置に固定座標が決められているとは限らないので乱数を用いているため, また動かせることによるメリットは, 視覚化における見やすさの向上のためであるが, 今後は不必要になる可能性もあります.

Q2:実行図のプログラムにあるオブジェクトの中身について.(松澤教授)

A2:今のプログラムにあるオブジェクトについては純粋にオブジェクトの繋がりしか読み込んでおらず, 推論するために必要な要素を取り込んでいません.